RECEIVED
CENTRAL FAX CENTER
OCT 2 4 2005

CERTIFICATE OF TRANSMISSION BY FACSIMILE (37 CFR 1.8) Applicant(s): Bickford et al.			Docket No. RSW920010143US1
Application No. 09/919,248	Filing Date 7/31/2001	Examiner Pyzocha, Michael J.	Group Art Unit 2137

Invention: AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL

I hereby certify that this Appeal Brief (30 pages with Transmittal)
(Identify type of correspondence)
is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No. 571-273-8300

on 10/24/2005
(Date)

Kim Dwileski
(Typed or Printed Name of Person Signing Certificate)

Kim Dwileski
(Signature)

Note: Each paper must have its own certificate of mailing.

RECEIVED
OIPE/IAP
OCT 2 4 2005

RECEIVED
CENTRAL FAX CENTER
OCT 24 2005

DOCKET NO.: RSW920010143US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.*	Examiner: Pyzocha, Michael J.
Serial No.: 09/919,248	Art Unit: 2137
Filed: 07/31/2001	

Title: AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANT

This Appeal Brief, pursuant to the Notice of Appeal filed August 22, 2005, is an appeal from the rejection of the Examiner in the final office action dated May 20, 2005.

REAL PARTY IN INTEREST

International Business Machines, Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 3-14 are rejected. Claims 1-2 are canceled.

STATUS OF AMENDMENTS

Appellants' response filed July 18, 2005 to the final office action amended claims 13 and 14. The Examiner's Advisory Action mailed August 5, 2005 states: "It is also noted that the amendments to claims 13 and 14 over come the rejections under 35 USC second paragraph for lack of antecedent basis." There are no other after-final amendments.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides an authentication method for electronic mail, comprising the steps of: preparing electronic mail for sending from an originator to a recipient; reading from a memory an authentication key associated with the originator; including the authentication key in an open field of the electronic mail; and sending the electronic mail from the originator to the recipient. See specification, page 7, lines 4-17. The electronic mail may have a subject line, and the open field of the electronic mail may be the subject line. See specification, page 7, lines 12-15. The authentication key may be associated with the originator may be further associated with the recipient. See specification, page 6, lines 8-17.

The present invention provides an authentication method for electronic mail, comprising the steps of: receiving electronic mail from an originator; determining whether an authentication key is present in an open field of the electronic mail; when an authentication key is present,

determining whether the authentication key is associated with the originator; and rejecting the electronic mail when the authentication key is not associated with the originator. See specification, page 7, line 17 - page 9, line 4. The open field of the electronic mail may be a subject line of the electronic mail. See specification, page 7, lines 12-15.

The present invention provides an authentication method for electronic mail, comprising the steps of: receiving electronic mail from an originator; determining whether an authentication key is expected to be present in an open field of the electronic mail; when an authentication key is expected to be present, determining whether the authentication key is associated with the originator; and rejecting the electronic mail when the authentication key is not associated with the originator. See specification, page 7, line 17 - page 9, line 4.

The present invention provides an authentication method for electronic mail, comprising the steps of: receiving electronic mail from an originator; determining whether an authentication key is expected to be present in an open field of the electronic mail; when an authentication key is expected to be present, determining whether the authentication key is present; when the authentication key is not present, rejecting the electronic mail; and when the authentication key is present, determining whether the authentication key is associated with the originator, accepting the electronic mail when the authentication key is associated with the originator, and rejecting the electronic mail when the authentication key is not associated with the originator. See

specification, page 7, line 17 - page 9, line 4. The step of determining whether an authentication key is expected to be present in an open field of the electronic mail may further include the step of reading a memory at an address that is dependent upon a source identifier that identifies the originator. See specification, page 7, line 18 - page 8, line 3; page 8, lines 10-11. The step of determining whether the authentication key is associated with the originator may further include the step of reading a memory at an address that is dependent upon a source identifier that identifies the originator. See specification, page 8, lines 13-20.

The present invention provides an authentication method for electronic mail, comprising the steps of: preparing electronic mail for sending from an originator to a recipient; sending the electronic mail from the originator to the recipient; receiving the electronic mail from the originator; determining whether an authentication key is present in an open field of the electronic mail; when an authentication key is present in the open field, determining whether the authentication key present in the open field is associated with the originator; and rejecting the electronic mail when the authentication key is not associated with the originator. See specification, page 7, line 17 - page 9, line 4.

The present invention provides an authentication method for electronic mail, comprising the steps of: receiving the electronic mail from an originator, the electronic mail having been previously prepared for sending from the originator to a recipient; determining whether an

authentication key is expected to be present in an open field of the electronic mail; when an authentication key is expected to be present, determining whether the authentication key is present; and rejecting the electronic mail when the authentication key is not present in the open field of the electronic mail. See specification, page 7, line 17 - page 8, line 12.

The present invention provides an authentication method for electronic mail having a subject line, comprising the steps of: receiving the electronic mail from an originator, the electronic mail having been previously prepared for sending from the originator with a source identifier to a recipient with a destination identifier; determining whether an authentication key is expected to be present in an open field of the electronic mail; when the authentication key is not expected to be present, accepting the electronic mail; when the authentication key is expected to be present, determining whether the authentication key is present; when the authentication key is present, determining whether the authentication key is associated with the originator and further associated with the recipient; accepting the electronic mail when the authentication key is determined to be associated with the originator and the recipient; rejecting the electronic mail when the authentication key is determined not to be associated with the originator and further associated with the recipient; and when the authentication key is not present, rejecting the electronic mail.. See specification, page 7, line 17 - page 9, line 4; page 6, lines 8-17.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 3-5 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Fischer and further in view of Bando et al (US 6,405,244).

2. Claims 6-7 and 12 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the modified Fischer and Bando et al system and further in view of Davis et al (US 5,937,160).

3. Claims 8-11 and 13-14 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the modified Fischer, Bando et al, and Davis et al system and further in view of MSA (post by Arthur Urbanowicz).

ARGUMENT

GROUND OF REJECTION 1

Claims 3-5 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Fischer and further in view of Bando et al (US 6,405,244).

Appellants respectfully contend that claim 3 is not unpatentable over Fischer in view of Bando, because Fischer and further in view of Bando does not teach or suggest each and every feature of claim 3. For example, Fischer and further in view of Bando does not teach or suggest the feature: "reading from a memory **an authentication key** associated with the originator; including **the authentication key** in an open field of the electronic mail" (emphasis added).

The Examiner argues: "Fischer fails to disclose reading from a memory an authentication key associated with the originator. However, Bando et al teaches reading authentication information associated with the originator (see column 5 line 54 through column 6 line 6)."

In response, Appellants respectfully contend that the Examiner's argument has neglected the fact that "the authentication key" in the "including" step has antecedent basis in "an authentication key" in the "reading" step. In other words, claim 3 requires that the authentication key that is read from memory is the **same key** that is stored in an open field of the electronic mail, which neither Fischer nor Bando teaches. The Examiner has acknowledged that Fischer does not teach the preceding feature of claim 3. Appellants contend that Bando does not teach the preceding feature of claim 3, because Bando's private key stored in memory is used only to generate a digital signature. See Bando, col. 5, line 62 - col. 6, line 6 explaining that the sender

uses a private key to generate a digital signature and the digital signature, and not the private key, is attached to the electronic mail. Bando does not teach or suggest that the private key used to generate a digital signature is also included in an open field of the electronic mail. In fact, if Bando's private key were also included in an open field of the electronic mail, the Bando's private key would no longer be "private".

In the Advisory Action mailed 08/05/2005, the Examiner argues that "in the combination, the authentication information of Fischer is the authentication key of Bando, which is associated with the originator because a public/private key pair is confidential to each individual."

In response to the preceding argument by the Examiner in the Advisory Action, Appellants respectfully contend that the Examiner is incorrect because in a private/public key authentication method, if the sender encrypts the message with the private key then the receiver decrypts the received message with the public key, wherein the private key is known only to the sender and not to the receiver. See Bando, col. 5, line 62 - col. 6, line 6 explaining that the sender uses a private key to generate a digital signature and the digital signature, and not the private key, is attached to the electronic mail; Bando further explains that the receiver decodes the received digital signature using the public key and not the private key.

See also, United States Patent 6,081,610 (Dwork et al., issued June 27, 2000) in col. 3, lines 6-17 reciting: "a signature is generated for a document, using a secret key. The secret key is preferably implemented as per the well-known public/private key system of RSA Data Security, which is well-known in the field of cryptography. In such a system, a given customer is assigned

a unique secret key, having a public key and a private key component.... **It is a characteristic of the key components that, if either one is used to encrypt a plaintext message, the other decodes the encrypted message.** Further, given the public key component, it is computationally infeasible to generate the private key component.... Therefore, a sender can encrypt a message intended only for the eyes of a recipient, using a recipient's public key, and send the encrypted message, knowing that only the recipient has the private key necessary to decrypt the message. On the other hand, a sender can encrypt a message using the sender's private key, so that any recipient who decrypts the message using the sender's public key knows that the message must have originated from the sender, because only the sender has the sender's private key." (emphasis added)

Since the Examiner has not demonstrated that the prior art teaches or suggests including an authentication key read from memory being included in an open field of the electronic mail, Appellants respectfully contend that the Examiner has not established a *prima facie* case of obviousness in relation to claim 3.

Based on the preceding arguments, Appellants respectfully maintain that claim 3 is not unpatentable over Fischer in view of Bando, and that claim 3 is in condition for allowance. Since claims 4-5 depend from claim 3, Appellants contend that claims 4-5 are likewise in condition for allowance.

In addition with respect to claim 5, Fischer and further in view of Bando does not teach or

suggest the feature: "wherein the authentication key associated with the originator is further associated with the recipient".

The Examiner agues: "As per claim 5, the modified Fischer and Bando et al system discloses the authentication key associated with the originator is further associated with the recipient (see Fischer paragraph 25) ."

In response, Appellants note that Par. 0025 of Fischer states that "Preferably, the vendor applies some level of security control when such e-mail order information is received and processed on behalf of a user... With vendors for whom the e-mail does not define the user's identity, then the user's transmission identity (e.g., e-mail address) can be used as corroborating evidence, with the user's identity being indicated elsewhere in the transmitted material. In either case, it may desirable for additional corroborating evidence of the user's identity, authentication or authorization, such as a "password", to be contained within the transmission."

The preceding quote from Par. 0025 of Fischer discloses associating the authenticating information with the user who is the sender and not the recipient of the e-mail order information. In Par. 0025 of Fischer, the vendor (and not the user) is the recipient of the e-mail order information. Therefore, Par. 0025 of Fischer has no relevance to the preceding feature of claim 5.

Accordingly, Appellants contend that the Examiner has not established a *prima facie* case of obviousness in relation to claim 5.

GROUND OF REJECTION 2

Claims 6-7 and 12 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the modified Fischer and Bando et al system and further in view of Davis et al (US 5,937,160).

The Examiner rejected claims 6-7 under 35 U.S.C. §103(a) as allegedly being unpatentable over the modified Fischer and Bando et al system and further in view of Davis et al (US 5,937,160).

Appellants respectfully contend that claims 6 and 12 are not unpatentable over the modified Fischer and Bando system and further in view of Davis, because the modified Fischer and Bando system and further in view of Davis does not teach or suggest each and every feature of claims 6 and 12.

A first example of why that claims 6 and 12 are not unpatentable over the modified Fischer and Bando system and further in view of Davis is that the modified Fischer and Bando system and further in view of Davis does not teach or suggest the feature: "determining whether an authentication key is present in an open field of the electronic mail" (emphasis added).

The Examiner argues: "The modified Fischer and Bando et al system fails to disclose determining whether an authentication key is present in an open field of the electronic mail. Davis et al teaches determining whether a type of information is present in an open field of the electronic mail (see column 11 lines 25-42). At the time of the invention it would have been

obvious to a person of ordinary skill in the art to use Davis et al's method of determining the presence of information in the subject field to determine if the authentication information of the modified Fischer and Bando et al system is present. Motivation to do so would have been to allow for different actions to occur based on the information in the subject (see Davis et al column 11 lines 25-42)."

In response, Appellants contend that the Examiner's preceding argument relating to Davis is not persuasive, because the authentication key in the open field of an electronic mail is not analogous to the information (i.e., a web page identifier) in an electronic mail pertaining to Davis, with respect to allowing for"different actions" (i.e., alternative actions) to occur. In Davis, col. 11 lines 25-42, the different actions based on the presence or absence of the web page identifier comprise saving the web page identifier if the web page identifier is present in the "Subject" field of the electronic mail, which makes sense since a web page identifier can be used to link to a web page. In contrast, an authentication key is of value for its functionality of authentication and not for its actual content. The Examiner has not provided any evidence from the prior art indicating that an authentication key could be beneficially utilized for its content in addition to its authentication functionality. Therefore, Appellants contend that it is not obvious to modify Fischer and Bando to perform the step of determining whether the authentication key is present in an open field of the electronic mail.

A second example of why that claims 6 and 12 are not unpatentable over the modified

Fischer and Bando system and further in view of Davis is that the modified Fischer and Bando system and further in view of Davis does not teach or suggest the feature: "rejecting the electronic mail when the authentication key is not associated with the originator".

The Examiner argues that the preceding feature of claims 6 and 12 are disclosed in Fischer and Bando. Appellants disagree and assert that neither Fischer nor Bando discloses "rejecting the electronic mail when the authentication key is not associated with the originator".

In Fischer's discussion of authentication of the user in Pars. 0025 and 0026, there no teaching or suggestion of "rejecting the electronic mail when the authentication key is not associated with the originator". Fischer, Pars. 0025 and 0026, discusses methods of authentication, but does not in any manner teach or suggest rejecting the electronic mail if the authentication key is not associated with the originator.

Likewise, in Bando's discussion of authentication in col. 5, line 54 - col. 6, line 6, there no teaching or suggestion of "rejecting the electronic mail when the authentication key is not associated with the originator". Bando, col. 5, line 54 - col. 6, line 6, discusses use of a private/public key system for generating and authenticating a digital signature, but does not in any manner teach or suggest rejecting the electronic mail if the authentication key is not associated with the originator.

Based on the preceding arguments, Appellants respectfully maintain that claims 6 and 12 are not unpatentable over the modified Fischer and Bando system and further in view of Davis,

and that claims 6 and 12 are in condition for allowance. Since claim 7 depends from claim 6, Appellants contend that claim 7 is likewise in condition for allowance.

GROUND OF REJECTION 3

Claims 8-11 and 13-14 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the modified Fischer, Bando et al, and Davis et al system and further in view of MSA (post by Arthur Urbanowicz).

The Examiner rejected claims 8-11 and 13-14 under 35 U.S.C. §103(a) as allegedly being unpatentable over the modified Fischer, Bando et al, and Davis et al system and further in view of MSA (post by Arthur Urbanowicz).

Appellants respectfully contend that claim 8 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, because the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest each and every feature of claim 8. For example, the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest the features: "determining whether an authentication key is expected to be present in an open field of the electronic mail".

The Examiner alleges that page 1, item 1 of MSA discloses the preceding features of claim 8. However, Appellants respectfully contend that the preceding feature of claim 8 does not exist on page 1, item 1 of MSA. In fact, the conditional determination required by claim 8 is not disclosed on page 1, item 1 of MSA. The only conditional action recited in Indeed, MSA, page 1, item 1 is: "When enabled, the smtserver *requires* the users outside the trusted network to authenticate themselves", which is not a conditional determination of whether an authentication key is expected to be present in an open field of the electronic mail, as required by claim 8.

Based on the preceding arguments, Appellants respectfully maintain that claim 8 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, and that claim 8 is in condition for allowance.

Appellants respectfully contend that claim 9 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, because the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest each and every feature of claim 9. For example, the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest the feature: "determining whether an authentication key is expected to be present in an open field of the electronic mail". The Examiner relies on the Examiner's argument, based on MSA, for the same feature of claim 8. In response, Appellants rely on Appellants' argument *supra* traversing the Examiner's argument for the same feature of claim 8.

In addition, Appellants respectfully contend that , the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest the feature: "rejecting the electronic mail when the authentication key is not associated with the originator." The preceding feature also appears in claims 6 and 12, and Appellants make reference to Appellants' discussion *supra* in arguing that Fischer and Bando system and further in view of Davis does not teach or suggest the feature: "rejecting the electronic mail when the authentication key is not associated with the originator." Appellants note that the Examiner has not even addressed the preceding feature in

relation to claim 9 and therefore not established a *prima facie* case of obviousness in relation to claim 9.

In addition, Appellants respectfully contend that , the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest the feature: "when the authentication key is not present, rejecting the electronic mail." The Examiner has not even addressed the preceding feature of claim 9 and has therefore not established a *prima facie* case of obviousness in relation to claim 9.

Based on the preceding arguments, Appellants respectfully maintain that claim 8 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, and that claim 9 is in condition for allowance. Since claims 10-11 depend from claim 9, Appellants contend that claims 10-11 are likewise in condition for allowance.

In addition with respect to claim 10, Appellants respectfully contend that Fischer, Bando, and Davis system and further in view of MSA does not disclose the feature: "reading a memory at an address that is dependent upon a source identifier that identifies the originator".

The Examiner argues: "see MSA where the trusted server name is inherently stored in memory".

In response, Appellants dispute the Examiner's contention that "the trusted server name is inherently stored in memory" is irrelevant, because the feature: "reading a memory at an address that is dependent upon a source identifier that identifies the originator" is not a logical

consequence of the Examiner's allegation that "the trusted server name is inherently stored in memory" (emphasis added).

In addition, Appellants maintain that inherency cannot be used to reject a claim under 35 U.S.C. § 103(a). *In re Shetty*, 566 F.2d 81, 86, 195 U.S.P.Q. 753, 756-57 (C.C.P.A. 1977) (reversing the Board's rejection of a claim based on alleged inherency under 35 U.S.C. 103 of a method to curb appetite, and stating: "[t]he inherency of an advantage and its obviousness are entirely different questions. That which may be inherent is not necessarily known. Obviousness cannot be predicated on what is unknown"). Therefore, the Examiner's arguments invoking inherency have no legal weight and are therefore not persuasive in relation to claim 10.

In addition with respect to claim 11, Appellants respectfully contend that Fischer, Bando, and Davis system and further in view of MSA does not disclose the feature: "reading a memory at an address that is dependent upon a source identifier that identifies the originator".

The Examiner argues that the preceding feature of claim 11 is disclosed in Bando, col. 5, line 54 - col. 6, line 6.

In response, Appellants dispute the Examiner's contention that the preceding feature of claim 11 is disclosed in Bando, col. 5, line 54 - col. 6, line 6. Indeed, Bando, col. 5, line 54 - col. 6, line 6 is totally silent as to said "address".

In "Response to Arguments", the Examiner argues: "an address is inherent to memory".

In response, Appellants dispute the Examiner's contention that "an address is inherent to

memory" is irrelevant, because the feature: "reading a memory at an address that is dependent upon a source identifier that identifies the originator" is not a logical consequence of the Examiner's allegation that "an address is inherent to memory".

In addition, Appellants maintain that inherency cannot be used to reject a claim under 35 U.S.C. § 103(a). *In re Shetty*, 566 F.2d 81, 86, 195 U.S.P.Q. 753, 756-57 (C.C.P.A. 1977) (reversing the Board's rejection of a claim based on alleged inherency under 35 U.S.C. 103 of a method to curb appetite, and stating: "[t]he inherency of an advantage and its obviousness are entirely different questions. That which may be inherent is not necessarily known. Obviousness cannot be predicated on what is unknown"). Therefore, the Examiner's arguments invoking inherency have no legal weight and are therefore not persuasive in relation to claim 11.

Appellants respectfully contend that claim 13 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, because the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest each and every feature of claim 13. For example, the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest the features: "determining whether an authentication key is expected to be present in an open field of the electronic mail; when an authentication key is expected to be present, determining whether the authentication key is present; and rejecting the electronic mail when the authentication key is not present in the open field of the electronic mail".

The Examiner relies on the Examiner's arguments relating to claims 12 and 9. In response, Appellants rely on Appellants' arguments relating to claims 12 and 9.

Based on the preceding arguments, Appellants respectfully maintain that claim 13 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, and that claim 13 is in condition for allowance.

Appellants respectfully contend that claim 14 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, because the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest each and every feature of claim 14. For example, the modified Fischer, Bando, and Davis system and further in view of MSA does not teach or suggest the features: "receiving the electronic mail from an originator, the electronic mail having been previously prepared for sending from the originator with a source identifier to the recipient with a destination identifier; determining whether an authentication key is expected to be present in an open field of the electronic mail; when the authentication key is not expected to be present, accepting the electronic mail; when the authentication key is expected to be present, determining whether the authentication key is present; when the authentication key is present, determining whether the authentication key is associated with the originator and further associated with the recipient; accepting the electronic mail when the authentication key is determined to be associated with the originator and the recipient; rejecting the electronic mail when the authentication key is determined not to be

associated with the originator and further associated with the recipient; and when the authentication key is not present, rejecting the electronic mail".

The Examiner argues: "see rejection of above claims where it is inherent that every email has a source and destination identifier". In "Response to Arguments" the Examiner further argues that "every email has a source and destination identifier as seen in RFC 822 each electronic mail has source and destination identifiers.".

In response, Appellants contend that the Examiner has made a statement without providing any analysis to connect the statement with the preceding features of claim 14. Thus, the Examiner's argument cannot be reasonably understood. Accordingly, the Examiner not established a *prima facie* case of obviousness in relation to claim 14.

In addition, Appellants maintain that inherency cannot be used to reject a claim under 35 U.S.C. § 103(a). *In re Shetty*, 566 F.2d 81, 86, 195 U.S.P.Q. 753, 756-57 (C.C.P.A. 1977) (reversing the Board's rejection of a claim based on alleged inherency under 35 U.S.C. 103 of a method to curb appetite, and stating: "[t]he inherency of an advantage and its obviousness are entirely different questions. That which may be inherent is not necessarily known. Obviousness cannot be predicated on what is unknown"). Therefore, the Examiner's arguments invoking inherency have no legal weight and are therefore not persuasive in relation to claim 14.

Based on the preceding arguments, Appellants respectfully maintain that claim 14 is not unpatentable over the modified Fischer, Bando, and Davis system and further in view of MSA, and that claim 14 is in condition for allowance.

SUMMARY

In summary, Appellant respectfully requests reversal of the May 20, 2005 Office Action rejection of claims 3-14.

Respectfully submitted,

Jack P. Friedman

Jack P. Friedman
Attorney For Appellant
Registration No. 44,688

Dated: 10/24/2005

Schmeiser, Olsen & Watts
3 Lear Jet Lane - Suite 201
Latham, New York 12110
(518) 220-1850

DOCKET NO.: RSW920010143US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.*	)	Examiner: Pyzocha, Michael J.
Serial No.: 09/919,248	)	Art Unit: 2137
Filed: 07/31/2001	)	

Title: AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX A - CLAIMS ON APPEAL

3. An authentication method for electronic mail, comprising the steps of:

preparing electronic mail for sending from an originator to a recipient;

reading from a memory an authentication key associated with the originator;

including the authentication key in an open field of the electronic mail; and

sending the electronic mail from the originator to the recipient.

4. The method of claim 3, wherein the electronic mail has a subject line, and the open field of the electronic mail is the subject line.

5. The method of claim 3, wherein the authentication key associated with the originator is further associated with the recipient.

6. An authentication method for electronic mail, comprising the steps of:

receiving electronic mail from an originator;

determining whether an authentication key is present in an open field of the electronic mail;

when an authentication key is present, determining whether the authentication key is associated with the originator; and

rejecting the electronic mail when the authentication key is not associated with the originator.

7. The method of claim 6, wherein the open field is a subject line of the electronic mail.

8. An authentication method for electronic mail, comprising the steps of:

receiving electronic mail from an originator;

determining whether an authentication key is expected to be present in an open field of the electronic mail;

when an authentication key is expected to be present, determining whether the authentication key is present; and

rejecting the electronic mail when the authentication key is not present.

9. An authentication method for electronic mail, comprising the steps of:

receiving electronic mail from an originator;

determining whether an authentication key is expected to be present in an open field of the electronic mail;

when an authentication key is expected to be present, determining whether the authentication key is present;

when the authentication key is not present, rejecting the electronic mail; and

when the authentication key is present, determining whether the authentication key is associated with the originator, accepting the electronic mail when the authentication key is associated with the originator, and rejecting the electronic mail when the authentication key is not associated with the originator.

10. The method of claim 9, wherein the step of determining whether an authentication key is expected to be present in an open field of the electronic mail further includes the step of reading a memory at an address that is dependent upon a source identifier that identifies the originator.

11. The method of claim 9, wherein the step of determining whether the authentication key is associated with the originator further includes the step of reading a memory at an address that is dependent upon a source identifier that identifies the originator.

12. An authentication method for electronic mail, comprising the steps of:

preparing electronic mail for sending from an originator to a recipient;

sending the electronic mail from the originator to the recipient;

receiving the electronic mail from the originator;

determining whether an authentication key is present in an open field of the electronic mail;

when an authentication key is present in the open field, determining whether the authentication key present in the open field is associated with the originator; and

rejecting the electronic mail when the authentication key is not associated with the originator.

13. An authentication method for electronic mail, comprising the steps of:

receiving the electronic mail from an originator, the electronic mail having been previously prepared for sending from the originator to a recipient;

determining whether an authentication key is expected to be present in an open field of the electronic mail;

when an authentication key is expected to be present, determining whether the authentication key is present; and

rejecting the electronic mail when the authentication key is not present in the open field of the electronic mail.

14. An authentication method for electronic mail having a subject line, comprising the steps of:

receiving the electronic mail from an originator, the electronic mail having been previously prepared for sending from the originator with a source identifier to a recipient with a destination identifier;

determining whether an authentication key is expected to be present in an open field of

the electronic mail;

when the authentication key is not expected to be present, accepting the electronic mail;

when the authentication key is expected to be present, determining whether the authentication key is present;

when the authentication key is present, determining whether the authentication key is associated with the originator and further associated with the recipient;

accepting the electronic mail when the authentication key is determined to be associated with the originator and the recipient;

rejecting the electronic mail when the authentication key is determined not to be associated with the originator and further associated with the recipient; and

when the authentication key is not present, rejecting the electronic mail.

RECEIVED
CENTRAL FAX CENTER
OCT 2 4 2005

DOCKET NO.: RSW920010143US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.*	)	Examiner: Pyzocha, Michael J.
Serial No.: 09/919,248	)	Art Unit: 2137
Filed: 07/31/2001	)	

Title: AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX B - EVIDENCE

There is no evidence entered by the Examiner and relied upon by Appellant in this appeal.

RECEIVED
CENTRAL FAX CENTER
OCT 2 4 2005

DOCKET NO.: RSW920010143US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Bickford *et al.*	)	Examiner: Pyzocha, Michael J.
Serial No.: 09/919,248	)	Art Unit: 2137
Filed: 07/31/2001	)	

Title: AUTHENTICATING WITHOUT OPENING ELECTRONIC MAIL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPENDIX C - RELATED PROCEEDINGS

There are no proceedings identified in the "Related Appeals and Interferences" section.